ThreatModeler
Security by Design

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2017

Electrical Substation ICS - 1

06/18/2017

Threats

Threat	Source	Risk	Status	Date Created
Denial of Service	Digital Relay	Very High	Open	06/18/2017
Denial of Service	RTU	Very High	Open	06/18/2017
Targeted Malware	Digital Relay	Very High	Open	06/18/2017
Exploitation of Authorization	PLC	Medium	Open	06/18/2017
Denial of Service	PLC	Very High	Open	06/18/2017
Jamming	RTU	Very High	Open	06/18/2017
File Manipulation	Monitor Station	Medium	Open	06/18/2017
Social Engineering Attacks	PLC	Low	Open	06/18/2017
Fuzzing	PLC	Medium	Open	06/18/2017
Windows ::DATA Alternate Data Stream	Monitor Station	Medium	Open	06/18/2017
Exploiting Incorrectly Configured Access Control Security Levels	Monitor Station	Medium	Open	06/18/2017
Group Permission Footprinting	Monitor Station	Very High	Open	06/18/2017
File Manipulation	Engineering Workstation	Medium	Open	06/18/2017
Windows ::DATA Alternate Data Stream	Engineering Workstation	Medium	Open	06/18/2017
Exploiting Incorrectly Configured Access Control Security Levels	Engineering Workstation	Medium	Open	06/18/2017

Exploiting Incorrectly Configured SSL Security Levels	Engineering Workstation	Low	Open	06/18/2017
TCP Window Scan	Engineering Workstation	Low	Open	06/18/2017
Windows Admin Shares with Stolen Credentials	Engineering Workstation	Very High	Open	06/18/2017
Group Permission Footprinting	Engineering Workstation	Very High	Open	06/18/2017
File Manipulation	OPC Server	Medium	Open	06/18/2017
Windows ::DATA Alternate Data Stream	OPC Server	Medium	Open	06/18/2017
Exploiting Incorrectly Configured Access Control Security Levels	OPC Server	Medium	Open	06/18/2017
Exploiting Incorrectly Configured SSL Security Levels	OPC Server	Low	Open	06/18/2017
TCP Window Scan	OPC Server	Low	Open	06/18/2017
Windows Admin Shares with Stolen Credentials	OPC Server	Very High	Open	06/18/2017
Group Permission Footprinting	OPC Server	Very High	Open	06/18/2017
Jamming	Slave IEC	Very High	Open	06/18/2017
Denial of Service	Slave IEC	Very High	Open	06/18/2017
Jamming	Master IEC	Very High	Open	06/18/2017
Denial of Service	Master IEC	Very High	Open	06/18/2017
Exploiting Incorrectly Configured SSL Security Levels	Monitor Station	Low	Open	06/18/2017
TCP Window Scan	Monitor Station	Low	Open	06/18/2017
Denial of Service	Router	Very High	Open	06/18/2017
Windows Admin Shares with Stolen Credentials	Monitor Station	Very High	Open	06/18/2017
Authentication Bypass	Router	Medium	Open	06/18/2017
Exploit Common and or default Usernames and Passwords	Router	High	Open	06/18/2017
DNS Cache Poisoning	Internet	Very High	Open	06/18/2017
Eavesdropping	Router	Very High	Open	06/18/2017
IP Spoofing	Router	High	Open	06/18/2017
Character Injection	Internet	Medium	Open	06/18/2017

Denial of Service	Internet	Very High	Open	06/18/2017
Identity Spoofing - Impersonation	Internet	Medium	Open	06/18/2017
Using UTF-8 Encoding to Bypass Validation Logic	Internet	High	Open	06/18/2017
HTTP Parameter Pollution	Internet	Very High	Open	06/18/2017
Sniffing Attacks	Ethernet	Medium	Open	06/18/2017
TCP ACK Ping	Ethernet	Low	Open	06/18/2017
TCP Window Scan	Ethernet	Low	Open	06/18/2017
TCP RPC Scan	Ethernet	Low	Open	06/18/2017
TCP FIN scan	Ethernet	Low	Open	06/18/2017
TCP SYN Scan	Ethernet	Low	Open	06/18/2017
TCP Null Scan	Ethernet	Low	Open	06/18/2017
TCP Sequence Number Probe	Ethernet	Low	Open	06/18/2017
TCP ISN Greatest Common Divisor Probe	Ethernet	Low	Open	06/18/2017
TCP ISN Sequence Predictability Probe	Ethernet	Low	Open	06/18/2017
TCP ISN Counter Rate Probe	Ethernet	Low	Open	06/18/2017
Targeted Malware	Ethernet	Very High	Open	06/18/2017
TCP Congestion Control Flag ECN Probe	Ethernet	Low	Open	06/18/2017
TCP Initial Window Size Probe	Ethernet	Low	Open	06/18/2017
TCP Flood	Ethernet	Very High	Open	06/18/2017
Malware-Directed Internal Reconnaissance	OPC - DA	Very High	Open	06/18/2017